

REMARKS

Claims 1-23 are pending in the patent application. The Examiner has rejected Claims 2, 4, 6, 8, 10, 12, and 20 under 35 USC 102 as anticipated by the Feldman article. The Examiner has indicated that Claims 1, 3, 5, 7, 9, 11, 13-19, and 21-23 are allowed.

The invention as recited in the rejected claims is directed to a method and program storage device for achieving agreement among n participating network devices to a first or second agree-value in an asynchronous network, the agreement arising out of a series of messages being sent and received with a signature by each participating network device, whereby the number t of faulty devices is less than $n/3$. The method comprises the steps of: broadcasting to all participating network devices a pre-vote value; performing a main-vote to amplify majorities if $n - t$ pre-vote values are validly received; broadcasting a main-vote value to all participating network devices; deciding for the first or second agree-value based on the received main-vote values; broadcasting a share-value to open a cryptographic common coin to all participating network devices; receiving share-values and assembling out of those a common value; uncovering a bit out of the common value, and, repeating the steps using the bit as the pre-vote value if the pre-vote values were different. Applicants have amended the language of Claims 2 and 20 to now recite receiving k share-values and, where $k > t$, assembling out of those a common value, uncovering a bit out of the common value, comparing the bit to the pre-vote value and

CH919990046-US1

-13-

repeating the steps starting from i) using the bit as the pre-vote value if the pre-vote values were different.

Applicants respectfully assert that the claim language, as amended, is patentable over the Feldman article. Applicants also believe that the amended claim language is consistent with the Examiner's statement of *Allowable Subject Matter* as set forth in paragraph 5 at the top of page 4 of the Office Action. The Examiner provided the following statement of reasons for the indication of allowable subject matter, "[i]t was not found to be taught in the prior art of broadcasting a shared value to participating network devices to generate an unpredictable bit, receiving k share values from the participating network devices, where k is larger than t , assembling out of those a common value and a deriving [a] bit" (*sic*). Applicants believe that Claim 2, Claims 4, 6, 8, 10, and 12 which depend from Claim 2, and Claim 20 now recite allowable subject matter.

Applicants also contend that the Feldman article does not anticipate the invention as claimed. The Feldman article is directed to "Optimal Algorithms for Byzantine Agreement" and provides that processors can reach Byzantine agreement "in an *asynchronous* network if any $< n/4$ faults occur" (see: the Abstract, page 148). Applicants disagree with the Examiner's statement that Feldman teaches achieving agreement in an asynchronous network having less than $n/3$ faulty devices. Feldman only concludes that for synchronous networks. Moreover, the Feldman article does not teach the claimed steps for achieving agreement. Feldman teaches, in the cited passage on page 148, section 1.1, the same prior art discussed by the present Specification. Applicants

CH919990046-US1

-14-

have described the drawbacks of the prior approaches and will not reiterate those arguments herein, since Applicants are not claiming that which is old. With regard to the cited passage from pages 150-151, Applicants note that Feldman does teach secret sharing wherein each network device receives a different part of the shared secret. The Feldman passage does not teach or suggest the use of a pre-vote to arrive at a first or second agree-value based on received main-vote values, the broadcasting of one share-value to all devices, and the use of that one broadcast share-value as set forth in the receiving/assembling/uncovering step in all of the rejected claims. Similarly, the cited passage from page 156, section 4.3 through section 4.4 of Feldman does not teach the invention as claimed. In sections 4.3 and 4.4, Feldman details the sending of a private input B_i for each device, which input is part of the shared secret (see: e.g., page 156, column 2, paragraph 3 and page 157, column 2, line 2). Alternatively, on page 158, column 2, for the *Vote* protocol, Feldman teaches that each device randomly and independently chooses its private input, s_{ij} . Clearly the Feldman article does not teach that the same share-value be provided to each device, as is taught and claimed by the present invention. Accordingly, Applicants conclude that the Feldman patent does not anticipate the invention as claimed.

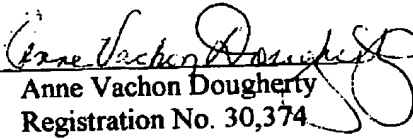
It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Feldman article does not teach steps or means for achieving agreement among device including the claimed steps of broadcasting to all participating network devices a

pre-vote value; performing a main-vote to amplify majorities if $n - t$ pre-vote values are validly received; broadcasting a main-vote value to all participating network devices; deciding for the first or second agree-value based on the received main-vote values; broadcasting a share-value to open a cryptographic common coin to all participating network devices; receiving k share-values and, where $k > t$, assembling out of those a common value, uncovering a bit out of the common value, comparing the bit to the pre-vote value and repeating the steps starting from i) using the bit as the pre-vote value if the pre-vote values were different, it cannot be maintained that Feldman anticipates the invention as set forth in the independent Claim 2, Claims 4, 6, 8, 10, and 12 which depend therefrom and add further limitations thereto, and Claim 20.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

K. Kursawe, et al

By: 
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910

CH919990046-US1

-16-